IN THE CLAIMS:

Applicant respectfully requests that the Claims of the above-identified application be amended so as to read as follows so as to place the same in condition for allowance, or at least in better form for Appeal, pursuant to 37 CFR 1.116:

1. (Currently Amended) An anti-tampering signature ~~method~~ comprising ~~method~~ method comprising the steps of:

providing a rewriteable ~~media~~ medium including (i) an information display area wherein display data is stored in a visually viewable, rewritable and erasable state, (ii) a plurality of display data certifier identification areas wherein display data certifier signature information is stored in a visually viewable, rewritable and erasable state; and (iii) a plurality of certification data areas corresponding respectively to each said certifier identification ~~areas~~ area for displaying and storing ~~wherein~~ certification data ~~associated~~ respectively indicates a registration status of an associated ~~with each~~ certifier signature information ~~is respectively stored~~ in a visually viewable, rewritable and erasable state;

determining whether or not said certifier signature information contained in each of said plurality of display data certifier identification areas, or to be added to one or more of said display data certifier identification areas, matches with corresponding registered certifier signature information stored in, or separately added to, a registered certifier signature information database, and, in those cases wherein a match is judged to be present, adding said registration status of said certifier signature information to said certification data areas associated with the certifier identification area displaying said certifier signature information, and in those cases wherein a match is not judged to be present, issuing a warning that signature tampering may have occurred;

extracting as a characteristic quantity ~~that represents~~ a general characteristic of image data generated by reading the display data according to an instruction from a certifier who has certified the display data,

generating encrypted data by encrypting said characteristic quantity using an encryption key paired with an identifier,

appending each said identifier and its associated encrypted data to the rewritable medium in a certification data area corresponding to the certifier who issued the instruction for the extraction of the characteristic information,

obtaining the encryption key based on the identifier according to an instruction of a verifier who verifies a certificate,

decrypting the obtained characteristic quantity of ~~of~~ the display data, and

judging whether or not the decrypted characteristic quantity obtained by decrypting the encrypted data and the characteristic quantity of the display data match, and, in those cases wherein a match is not judged to be present, issuing a warning that signature tampering may have occurred.

2. (Canceled)

3. (Currently Amended) An anti-tampering signature apparatus for executing an anti-tampering signature method comprising:

a rewriteable ~~media~~ medium including (i) an information display area wherein display data is stored in visually viewable, rewritable and erasable state, (ii) a plurality of display data certifier identification areas wherein display data certifier signature information is stored in a visually viewable, rewritable and erasable state; and (iii) a plurality of certification data areas corresponding respectively to each said plurality of display data certifier identification ~~areas wherein~~ area for displaying and storing certification data ~~associated with each~~ respectively indicates a registration status of an associated certifier ~~is~~ signature information ~~respectively stored~~ in a visually viewable, rewritable and erasable state;

first tampering judgment means for determining whether or not said certifier signature information contained in each of said plurality of display data certifier identification areas, or to be added to one or more of said plurality of display data certifier identification areas, matches with corresponding registered certifier signature information stored in, or separately added to, a registered certifier signature information database, and for in those cases wherein a match is judged to be present, adding said registration status of said certifier signature information to said certification data areas associated with the certifier identification area displaying said certifier signature information, and in those cases wherein a match is not judged to be present, issuing a warning that signature tampering may have occurred;

said determination including:

characteristic quantity extraction means for extracting as a characteristic quantity ~~that represents~~ a ~~characteristic~~general characteristic of image data generated by reading the display data according to an instruction from a certifier who has certified the display data,

encryption / decryption means that generates encrypted data by encrypting said characteristic quantity using an encryption key paired with an identifier, and decrypts the encrypted data into said characteristic quantity,

appending means for appending each said identifier and its associated encrypted data to the rewritable medium in a certification data area corresponding to the certifier who issued the instruction for the extraction of the characteristic information, and

~~second tampering~~second tampering judgment means for judging whether or not the decrypted characteristic quantity and the characteristic quantity of the display data match, and, in those cases wherein a match is not judged to be present, issuing a warning that signature tampering may have occurred.

4. (Currently Amended) An anti-tampering signature system wherein display data is displayed on a rewritable medium including (~~i~~I) an information display area wherein display data is stored in a visually viewable, rewritable and erasable state, (ii) a plurality of display data certifier identification areas wherein display data certifier signature information is stored in a visually viewable, rewritable and erasable state; and (iii) a plurality of certification data areas corresponding respectively to each said plurality of display data certifier identification ~~areas wherein~~ area for displaying and storing certification data respectively indicates a registration status of an associated ~~with each~~ certifier signature information ~~is respectively stored~~ in a visually viewable, rewritable and erasable state is certified, comprising:

first tampering judgment means for determining whether or not said certifier signature information contained in each of said plurality of display data certifier identification areas, or to be added to one or more of said plurality of display data certifier identification areas, matches with corresponding registered certifier signature information stored in, or separately added to, a registered certifier signature information database, and for in those cases wherein a match is judged to be present, adding said registration status of said certifier signature information to said certification data areas associated with the certifier identification area displaying said certifier signature information, and in those cases wherein a match is not judged to be present, issuing a warning that signature tampering may have occurred;

encryption key generating means that registers an identifier and generates an encryption key,

storage means for storing the identifier and the encryption key,

certifying means that supplies the encryption key according to a query based on the identifier,

~~and~~

~~anti-tampering signature apparatus provided with a~~ characteristic quantity extraction means for extracting as a characteristic quantity ~~that represents~~ a general characteristic of image data generated by reading the display data according to an instruction from a certifier who has certified the display data,

encryption / decryption means that generates encrypted data by encrypting said characteristic quantity using an encryption key paired with an identifier and decrypts the encrypted data into said characteristic quantity,

appending means for appending each said identifier and its associated encrypted data to the rewritable medium in a certification data area corresponding to the certifier who issued the instruction for the extraction of the characteristic information, and

a second tampering judgment means for judging whether or not the decrypted characteristic quantity and the characteristic quantity of the display data match, and, in those cases wherein a match is not judged to be present, issuing a warning that signature tampering may have occurred.

5. (Canceled)

6. (Currently Amended) A computer-readable recording medium on which ~~the anti-tampering signature program according to claim 5 is recorded~~ is stored an anti-tampering signature program for causing a computer to perform an anti-tampering signature method with respect to a rewritable ~~media~~ medium including (~~i~~I) an information display area wherein display data is stored in a visually viewable, rewritable and erasable state, (ii) a plurality of display data certifier identification areas wherein display data certifier signature information is stored in a visually viewable, rewritable and erasable state; and (iii) a plurality of certification data areas corresponding respectively to each said certifier identification ~~areas wherein~~ area for displaying or storing certification data respectively indicates a registration status of an associated ~~associated with each~~ certifier signature information ~~is respectively stored~~ in a visually viewable, rewritable and erasable state, said anti-tampering signature program comprising the steps of:~~:~~

determining whether or not certifier signature information contained in said plurality of display data certifier identification areas, or to be added to, one or more of said plurality of display data certifier identification areas, matches with corresponding registered certifier signature information stored in, or separately added to, a registered certifier signature information database, and, in those cases wherein a match is judged to be present, adding said registration status of said certifier signature information to said certification data areas associated with the certifier identification area displaying said certifier signature information, and in those cases wherein a match is not judged to be present, issuing a warning that signature tampering may have occurred;

extracting as a characteristic quantity ~~that represents~~ a general characteristic of image data generated by reading the display data according to an instruction from a certifier who has certified the display data, generating encrypted data by encrypting said characteristic quantity using an encryption key paired with an identifier,

appending each said identifier and its associated encrypted data to the rewritable medium in a certification data area corresponding to the certifier who issued the instruction for the extraction of the characteristic information,

obtaining the encryption key based on the identifier according to an instruction of a verifier who verifies a certificate,

decrypting the obtained characteristic quantity of the display data, and

judging whether or not the decrypted characteristic quantity obtained by decrypting the encrypted data and the characteristic quantity of the display data match, and, in those cases wherein a match is not judged to be present, issuing a warning that signature tampering may have occurred